CLAIMS:

1. An access control method, including:

receiving an initial access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said initial access request; and

applying a rate limit for verifying access to said service until said identification data is verified by a user of said apparatus.

2. An access control method as claimed in claim 1, wherein verifying said identification data corresponds to a first level of access control, and said method includes applying at least one additional level of access control following a predetermined number of failed attempts to verify said identification data by said user of said apparatus.

3. An access control method as claimed in claim 2, wherein said identification data is a random unique security code and said apparatus is sent an unique identification number which expires if the security code is not verified within a predetermined period of time.

4. An access control method as claimed in claim 1, wherein said identification data is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide said identification data using said device.

5. An access control method as claimed in claim 1, wherein said identification data is verified by said user returning said identification data using communication means having a known association to said user and said data processing apparatus.

6. An access control method as claimed in claim 2, wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user.

7. An access control method as claimed in claim 2 or 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.

8. An access control method as claimed in claim 7, wherein said communication software encrypts said access requests.

9. An access control method as claimed in claim 2, including invoking sequentially the levels of access control depending on the number of failed attempts to verify said identification data by said user for access requests over predetermined periods of time.

10. An access control method as claimed in claim 7 when dependent on claim 6, wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

11. An access control method as claimed in claim 10, wherein said at least on additional level of access control includes a fourth level of access control involving blocking all access requests by said data processing apparatus.

12. An access control method as claimed in claim 11, wherein said blocking involves denying all access requests that include address data that corresponds to said data processing apparatus.

13. An access control method as claimed in claim 12, wherein the address data is an IP address or segment.

14. An access control method executed by a computer system, including:

applying an access rate limit until a user issuing access requests is verified;

a first control level involving verifying said user;

a second control level applying hack program detection tests to said access requests and verifying said user;

a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;

a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and

invoking said control levels sequentially depending on a number of failed attempts to verify said user.

15. An access control method as claimed in claim 14, wherein said user is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide identification data using said device.

16. An access control system having components for executing the steps of the access control method as claimed in any one of the preceding claims.

17. Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in any one of claims 1 to 15.

18. An access control system, including:

an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and

an IVR for contacting a device having an association with said data processing apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.